**IT Applications, Unit 4**

**Ch 8, Security and Ethical Considerations**

**Disaster Recovery Strategies, p 514**

1. What is a disaster recovery plan?

A document with steps needed to restore company operations in event of a disaster.

Preparing a disaster recovery plan:

1. List some considerations required in preparing a disaster recovery plan.

Store passwords in two separate secure locations, document the whole recovery process including location of recovery disks, establish an automated system to notify key staff of failures in the systems, practice the plan on a quarterly process, and build redundancy into the system, etc.

There are four key parts to a disaster recovery plan:

1. Preparing an emergency plan
   1. What should an emergency plan contain?

* Names & contact details of people to notify
* Procedures to follow with computer equipment
* Evacuation procedures for employees
* Return procedures

1. Preparing a “backup” plan
   1. What does a backup plan involve?

It covers the procedures that the company is to follow for using file backups to restore computer systems.

* 1. List what the plan should include
* Location of alternative sites & equipment
* Location of backup data, supplies, eq/ment
* Personnel responsible for gathering backup resources
* Schedule indicating order & approximate time applications up and running

1. Preparing a recovery plan
   1. What does a recovery plan involved?

It involves specific procedures for restoring the full information processing capacity of the organisation. It covers replacement of both hardware and software.

* 1. What are the things to consider when writing a recovery plan?
* Covers hardware & software replacement
* Identification of mission critical ICT services
* Use of a backup site

1. Test plan
   1. What is looked for in testing a disaster recovery strategy?

It should contain information about simulating a variety of disasters and different recovery needs. It should identify problems with the plan, which are then corrected.

**Evaluating information-management strategies,** p 517

Elaborate on each of the following four criteria to consider in evaluating information-management strategies:

1. integrity of data

Accuracy, reliability and timeliness in terms of storage, communication and disposal, accuracy, e.g. storage, it contains all data; communication, arrives accurately, no viruses; disposal, selected files deleted or copied.

1. security

Evaluate physical & software security, e.g. audit trails.

1. ease of retrieval

Observance of folder & file-naming conventions, backed up files need to be able to be restored.

1. currency of files

Regular backups, use of sequential file-naming conventions.